GREATEST COMMON DIVISOR

Let a and b be integers with at least one of them is nonzero, then the gcd of a and b or gcd (a, b) is the positive integer d satisfying the following:

a) $d|$a and $d|b$ (d divides a and d divides b)

b) If $c|a$ and $c|b$ then $c \leq d$.

Example 1: Find the gcd $(12{,}60)$

Solution: By ***Prime Factorization***, we have:

12				60
2				2
2	=	6	=	2
3				3
				5

Answer: The gcd $(12, 60) = 12$

a) $12|12$ and $12|60$

b) $6|12$ and $6|60$, with $6 < 12$

Relatively Prime

Two integers a and b, both are nonzero, are said to be relatively prime whenever gcd $(a, b) = 1$.

The gcd integers a and b can be written as ***linear combination*** where there exist integers x and y such that gcd $(a, b) = ax + by$

Example 2: $gcd\ (12, 60) \ = 12$

Solution: By ***Euclidean Algorithm***,

we have:

$$60 = 12(5) \ + \ 0 \ \rightarrow \ \text{gcd}\ (12, 60) = 12$$

And by ***Linear Combination***,

we have:

$$12 = 12(-4) + 60(1) \text{ where } -4, 1 \in \mathbb{Z}.$$

Corollary 1: If gcd $(a, b) = d$, then gcd $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof: Suppose gcd $(a, b) = d$. Then by definition of gcd it follows that $d|a$ and $d|b$ such that

$a = md$ and $b = nd$.

Since $d =$ gcd (a, b), then all the factors that a and b have in common is contained in d.

Therefore, m and n are relatively prime.

That is:

$$\text{gcd}\left(\frac{a}{d}, \frac{b}{d}\right) = \text{gcd}\left(\frac{md}{d}, \frac{nd}{d}\right) = \text{gcd}\,(m, n) = 1$$

Example 3: For gcd $(12, 60) = 12$ we have:

Solution: $\frac{12}{12} = 1$ and $\frac{60}{12} = 5$

Answer: The gcd $(1, 5) = 1$

Corollary 2: If $a|c$ and $b|c$, with gcd $(a, b) = 1$, then $ab|c$.

Proof: Suppose $a|c$ and $b|c$ where $a, b \neq 0$, with gcd $(a, b) = 1$. Then, we need to show that $ab|c$.

Since $a|c$ and $b|c$ with gcd $(a, b) = 1$, it follows that ***by definition of divisibility*** $c = ka$ and $c = lb$ where $k = lb$ $(k, lb \in \mathbb{Z})$.

So that:

- $c = ka$
- $c = (lb)a$ ***Substituting the value of k***

- $c = l(ba)$ **By Associative Property of Multiplication**
- $c = l(ab)$ **By Commutative Property of Multiplication**

Since $c = l(ab)$ where $l \in \mathbb{Z}$, then by ***definition of divisibility***, $ab|c$.

Example 4: We have $5|60$ and $6|60$. Then:

Solution: gcd $(5, 6) = 1$. Therefore,

$$5(6)|60$$

$$\Rightarrow 30|60 \quad \rightarrow \quad \text{For } 60 = 2(30)$$